

Department of State
Report on Privacy and Civil Liberties Activities
Section 803 of 9/11 Commission Act of 2007
Reporting Period July 1, 2018 – December 31, 2018

I. Introduction

In accordance with Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, 42 U.S.C. 2000ee-1 (hereinafter “Section 803”), the Department of State (“Department”) is herein reporting for the period of July 1, 2018 – December 31, 2018. Section 803 requires periodic reports on the discharge of the functions of the Department’s Privacy and Civil Liberties Officer (“PCLO”), including information on: (1) the number and types of reviews undertaken; (2) the type of advice provided and response given to such advice; (3) the number and nature of complaints received by the Department, agency, or element concerned for alleged violations; and (4) a summary of the disposition of such complaints, the reviews and inquiries conducted, and the impact of the activities of the PCLO. *See* 42 U.S.C. 2000ee-1(f).

The Under Secretary for Management serves as the Department’s PCLO. The PCLO is the principal advisor to the Secretary of State on the privacy and civil liberties implications of Department policies and regulations. The Deputy Assistant Secretary for Global Information Services serves as the Department’s Senior Agency Official for Privacy (“SAOP”). The SAOP has overall responsibility and accountability for ensuring that privacy protections are integrated into all Department programs, policies, and procedures. Many of the day-to-day privacy compliance activities are handled by the Department’s Privacy Office, under the supervision of the SAOP. The Privacy Office is comprised of full-time program analysts who are responsible for conducting privacy compliance reviews, training Department personnel, assisting with reporting functions, and managing privacy breaches. The Office of the Legal Adviser advises the SAOP, the Privacy Office, and other Department personnel on compliance with the Privacy Act of 1974, as amended, 5 U.S.C. 552a, and other applicable laws and policies, including those pertaining to civil liberties.

II. Privacy Reviews

The Department of State conducts reviews of information technology systems and programs to assess potential privacy risks. The types of reviews conducted during this reporting period include the following:

Privacy Impact Assessments (“PIAs”) are a requirement of Section 208 of the eGovernment Act of 2002. The PIA is used to identify and assess privacy risks throughout the development lifecycle of a system or program.

Systems of Records Notices (“SORNs”) are required by the Privacy Act of 1974. *See* 5 U.S.C. 552a(e)(4). A SORN describes the existence and character of a system of records, including the categories of individuals whose records are in the system; the categories of records; and the routine uses of the records.

Privacy Act Statements (“PASs”) are required by the Privacy Act of 1974. *See* 5 U.S.C. 552a(e)(3). The PAS, which must be on the form used to collect the information or on a separate form that the individual can retain, includes the authority for collecting the information; the principal purpose for which the information is intended to be used; the routine uses of the information; and the effects on the individual, if any, of not providing all or any part of the requested information.

Breach Response Plan (“BRP”) establishes governing policies and procedures for handling breaches of personally identifiable information (PII) at the Department of State. These policies and procedures are driven by Office of Management and Budget (OMB) directives and based on applicable laws, Presidential Directives, best practices, and lessons learned. The Department’s first BRP was originally developed 10 years ago and was recently revised in accordance with OMB’s Memorandum M-17-12. Most notably, this BRP includes an updated Breach Incident Form, updated procedures for major versus non-major breaches, post-breach evaluations to help identify lessons learned (such as tasks that could have been conducted more effectively and/or efficiently) and to help make improvements as appropriate. Lastly, the Department is conducting an annual tabletop exercise to test the breach response plan and to help ensure that key members understand their specific roles.

During the reporting period, the Department completed 19 PIAs and reviewed 20 additional PIAs which are pending completion. Included below is a summary of key PIAs for this reporting period. All published PIAs are available on the Privacy Office website, <http://www.state.gov/privacy/>

1. **PEPFAR Events & Meetings (PEPFAREM)** – The Office of the U.S. Global AIDS Coordinator and Health Diplomacy leads implementation of the U.S. President's Emergency Plan for AIDS Relief (PEPFAR), which is the iconic brand of U.S. government engagement in health, development, security, and diplomacy. The PEPFAR Events & Meetings PIA is part of a pilot project within the Department utilizing the Foreign Affairs Network (FAN), which is a portfolio of secure, cloud-based services that enable Department personnel to securely collaborate and share information with other federal government agency personnel. PEPFAR Events & Meetings PIA is the first PIA using the new FAN-specific PIA template and procedures.
2. **Consular Consolidated Database (CCD)** – The Bureau of Consular Affairs (CA) is responsible for the welfare and protection of U.S. citizens abroad, for the issuance of passports and other documentation to citizens and nationals, and for the protection of U.S. border security and the facilitation of legitimate travel to the United States. The CCD is a comprehensive data warehouse that stores current and archived visa and passport data from all of the Consular Affairs post databases around the world and, so, provides CA a near real-time aggregate of consular transaction activity collected domestically and from posts worldwide. Using a web portal interface, users, which include the Department, DHS, FBI, DOD, and other federal agencies’ personnel, can provide input into the visa and passport review and approval process.

3. **Government Retirement and Benefits (GRB)** – GRB is a unique system created by the Human Resources (HR) Bureau at the Department of State (DoS) to provide DoS HR Specialists with a suite of tools for assisting employees with their retirement and benefits decisions, while increasing productivity and lowering costs by providing the framework for organizing and managing a high volume caseload. Because of the sheer volume of information and personally identifiable information that GRB gathers from other information systems across the Department, it is covered by multiple System of Record Notices that describe how it gathers, stores, and disseminates that information.
4. **Integrated Security and Suitability System (IS3)** – The Bureau of Diplomatic Security (DS) acts as the law enforcement and security arm of the U.S. Department of State. IS3 is a new comprehensive system that supports all of the functions and activities associated with the processing of personnel security including the investigative process, reviewing existing data, updating existing records, gathering data, and making informed decisions (both positive and adverse) on eligibility, access, and suitability based on national and Department standards. In addition, IS3 will support record keeping requirements, management metrics, financial linkages, and litigation support needs that the above processes require. The new IS3 system will replace several legacy systems, reengineer and automate current legacy and paper-based processes, and provide a foundation for an interconnected, inter-agency security clearance management solution.

During the reporting period, the Department published one SORN, summarized below; rescinded one SORN, also summarized below; and reviewed 15 SORNs which are pending completion. All published SORNs are available on the Privacy Office website, <http://www.state.gov/privacy/>

1. **State-50, Family Liaison Office Records** – Information covered by State-50 is used to manage the Family Liaison Office's programs and to provide services to its clients in each of its major areas of interest: Family Member Employment, Naturalization, Education and Youth, Unaccompanied Tours, Community Liaison Office Program and Support Services. In addition, State-49, Skills Catalogue Records, was merged into State-50 because the records were very similar.
2. **Rescindment of State-12, Foreign Service Employee Locator/Notification Records**: Because the records were similar, the records in State-12 were consolidated earlier in 2018 under a modified State-40, Employee Contact Records; State-12 was subsequently rescinded.

During this reporting period, the Department completed the review and approval of 14 PASs and Confidentiality Statements. Included below are three key PASs or Confidentiality Statements for this reporting period.

1. **DS-234, Special Immigrant Visa Biodata Form** – In accordance with the Immigration and Nationality Act, the DS-234 form allows qualifying special immigrant visa applicants to request from the Department of State the provision of resettlement and placement benefits and assistance in determining the location in the United States in which the immigrant will be resettled. The Privacy Office worked with the Bureau of Population, Refugees, and Migration to review and approve this Confidentiality Statement.
2. **DS-2029, Consular Report of Birth Abroad of a Citizen of the United States of America** – A Consular Report of a Birth Abroad may be issued for any U.S. citizen child under the age of 18 who was born abroad to American parents and who acquired U.S. citizenship at birth. The application must be signed before a U.S. consular officer or designated military official and serves as proof of U.S. citizenship. The Privacy Office worked with the Bureau of Consular Affairs to review and renew approval of this PAS.
3. **DS-3077, Request for Entry into Children’s Passport Issuance Alert Program** – The Department offers services whereby a parent either involved in a custody dispute or having concerns that their child may be taken abroad by the other parent without their knowledge, can enroll that child in the Children’s Passport Issuance Alert Program (CPIAP). After the child’s name is entered into CPIAP using this form, the child’s name then carries a “C” CLASS hit, which can be viewed by all posts and passport agencies when a passport application is submitted for the child and a passport agency or consulate runs a name check. A passport cannot be issued with a “C” hit without first contacting the Children’s Issues Office in the Bureau of Consular Affairs for resolution. The Privacy Office worked with the Bureau of Consular Affairs to review and approve this PAS.

III. Advice, Training, and Awareness

The Privacy Office advised various offices throughout the Department in connection with the privacy reviews described above. This advice is reflected in the final versions of these PIAs, SORNs, and PASs. The Office of the Legal Adviser also advised in connection with PIAs, SORNs, and PASs during the reporting period, and its advice is also reflected in these documents. In addition to providing this advice, during the reporting period, the Privacy Office conducted the following privacy training:

Mandatory On-line Training

- **1,469**, or 61% of new Department personnel completed the distance learning training course, PA459, Protecting Personally Identifiable Information. The course is a one-time mandatory training for all employees who handle PII.
- **59,254**, or 98% of Department personnel (domestic and overseas) completed the distance learning training course, PS800, Cybersecurity Awareness, which includes a

dedicated privacy module. This course is required annually for all personnel who access the Department's network.

Other Training

- **Privacy Awareness Briefings** - The Privacy Office provided a range of privacy awareness briefings throughout the Department. Of note, privacy awareness training was provided to 735 Department personnel in Charleston, SC, most of whose job duties entail handling large amounts of PII. By training 23 contractors in the Visa Office, the Privacy Office continued to provide privacy awareness briefings to contractors, who have otherwise been unable to receive training. Training was provided to 10 Department personnel as part of new employee orientation. Additionally, the Privacy Office has started to host small training sessions with IT managers from various bureaus to emphasize the accurate documentation of privacy controls in Privacy Impact Assessments (PIAs) for IT systems.

IV. Privacy Complaints

For purposes of this report, a complaint is a written allegation (excluding complaints filed in litigation with the Department) submitted to the PCLO alleging a violation of privacy or civil liberties concerning the handling of personal information by the Department in the administration of Department programs and operations.

The Department has no complaints to report.

V. Summary of Disposition of Complaints, Reviews, and Inquiries Conducted, and Impact of the Activities of Privacy and Civil Liberties Officer

The Department has no additional information to report.